





2010-09

# The Profession of IT, Discussing Cyber Attack

Denning, Peter J.

Discussing Cyber Attack (with Dorothy Denning)(September 2010) Cyber attack, the other side of cyber defense, deserves a more open discussion than it has been getting.

DOI:10.1145/1810891.1810904

Peter J. Denning and Dorothy E. Denning

# The Profession of IT
# Discussing Cyber Attack

*Cyber attack—the other side of cyber defense—deserves a more open discussion than it has been getting.*

"Defend our networks!" is the new rallying cry in a time of rising concerns over cyber vulnerabilities. Malware, Trojan horses, computer system weaknesses, network vulnerabilities, intrusions, data theft, identity theft, malicious botnets, and critical infrastructure protection are under constant discussion. Computing professionals are called on daily to help with these problems. Cyber defense is the topic of hundreds of conferences and research papers every year.

By contrast, cyber attack, the flip side of defense, has been a touchy subject. Many people feel queasy when they hear their governments want to be in a position to launch cyber attacks. Most public discussions of cyber attack tend to focus on the "bad guys" (unauthorized individuals with malicious intent) who launch the attacks and the methods they use—all for the purpose of developing better defenses. Governments are quiet about not only their cyber attack methods and operations, but also the policies they follow. This secretiveness has fueled many fears that governments are up to things the citizens would disapprove.

Yet there is a growing international public discussion on cyber attack, promoted in part by reports of government activity in the area. The U.S. Department of Defense established the U.S. Cyber Command earlier this year to coordinate the cyber defense of military networks and to direct military cyber attacks. Other militaries are doing the same. Security experts Richard Clarke and Robert Knake believe that cyber attacks and cyber war are already under way.[1] Massive denial-of-service attacks against government sites in Estonia in 2001 and Georgia in 2008 led to charges that Russia was engaging in cyber warfare. China was blamed for infiltrating and stealing sensitive data from Google's network and other targets in 2009. Many believe that cyber espionage by government intelligence agencies is widespread.

**Defense Secretary Robert Gates addresses the audience with Gen. Kevin Chilton, commander, U.S. Strategic Command, and Gen. Keith Alexander, commander, U.S. Cyber Command, during the activation ceremony of U.S. Cyber Command on Fort Meade, MD, May 21, 2010.**

PHOTOGRAPH BY DEPARTMENT OF DEFENSE / CHERIE CULLEN

There is an important role for computer professionals in the discussions and other activities in this area. To point the direction, we will use a recent report on cyber attack from the National Research Council.[3] The report, which addresses the technical, policy, legal, and ethical dimensions of cyber attack, makes important distinctions that are useful to frame the discussion. While written for the U.S., it discusses the issue in a way that relates to many countries.

## Cyber Attack and Exploitation

Cyber attack refers to deliberate actions against data, software, or hardware in computer systems or networks. The actions may destroy, disrupt, degrade, or deny access.

**Computing technologies open many options and complexities that more casual users do not appreciate.**

Many governments' militaries and intelligence agencies are actively preparing to engage in cyber attacks, perhaps in conjunction with conventional attacks or counterattacks.

Cyber exploitation is another term in the discussions. It refers to intelligence-gathering rather than destructive activities. Cyber exploitation usually seeks the least intrusive, least detectable interventions into computing systems. The purpose is to acquire data without being seen or getting caught. Exploitation also refers to forensic recovery of data from discarded (or captured) laptops and storage media.

Both attack and exploitation require three things: access to a system or network, vulnerabilities in the accessed systems, and a payload. The access might be remote through the Internet or close-in through physical access. Vulnerabilities can appear in hardware, software, hardware-software interfaces, communication channels, configuration tables, users, and service providers. The payload is a program that performs actions once a vulnerability has been found and exercised. A payload might be a bot, data monitoring program, virus, worm, spyware, or Trojan horse; and it is likely to have remote access to the attacker's communication channels. The difference between attack and exploitation depends on the actions of the payload. An attack payload is destructive, an exploit payload is nondestructive. Often the differences are so subtle that the victim of a cyber operation may not be able to tell as it is happening which it is.

Cyber attack and exploitation are tools used in the service of larger ends. They offer a new range of capabilities to government that can be more humane and less collaterally damaging than their traditional "kinetic" predecessors. For example, a military operation may depend on disabling an adversary's radars scattered around a city; if a cyber attack could disable the radars, there would be no need to bomb the installations and suffer all the collateral damage those bombings would entail. An intelligence operation that can steal files remotely avoids risking the lives of its secret agents. However, people who would accept these ends might also worry about the same tools being used for other ends, such as a government agency spying on its citizens.

The NRC report discusses the technical, policy, and social aspects of cyber attack and exploit. It identifies complicated issues that must be resolved in such areas as the law of armed conflict, deterrence, and the dynamics of cyber attack. While the principles underlying the United Nations charter on the use of force and armed attack offer a good starting point for an international regime governing cyber attacks, they are difficult to apply to many cyber attacks. Traditional policies of deterrence by threat of overwhelming response are problematic in cyberspace because of the extreme difficulty of accurately identifying perpetrators. The dynamics of cyber attack are also poorly understood, including how to keep a cyber conflict from escalating out of control and how to terminate cyber conflict. The report recommends that these and other issues be discussed in an open, public debate.

### The Need for Technical Expertise

It's tempting for us to say that these issues look primarily legal, ethical, or political, and that we should let lawyers, ethicists, and politicians look after them. That reasoning is unsound. Computing technologies open many options and complexities that more casual users do not appreciate. Computing professional advice on the capabilities and limits of the technology is crucial to the formulation of sound policies, as well as the development of tools for attack, exploit, and defense.

A significant example of this occurred in 1985 when the U.S. government undertook the Strategic Defense Initiative (SDI), an automated missile

defense system. Many computing people initially declined to join the debate because they believed it was inherently political and they had little to offer. That changed with David Parnas's remarkable *Communications* article, "Software aspects of strategic defense systems,"[4] which set out for the first time the scientific framework of software engineering. Parnas showed that software engineering at the time was not capable of producing reliable control systems for missile defense. After that many computing professionals joined the debate to add their own experience and expertise with unreliable large, complex systems.

There are several other examples where political and legal issues depended on an understanding of the limits of computing technology, and computing professionals made important contributions to the debates. These included the move toward e-voting, cryptography policy, architecting the Internet for strong authentication, technologies to improve or impede anonymity, proposals to charge postage on email to stop spam, and network neutrality.

Cyber attack is on par with the strategic defense issue. The complex and subtle issues of cyber attack cannot be adequately resolved unless experts knowledgeable in the workings and capabilities of information technologies participate actively in the discussions. Some of the areas where technical expertise is essential include:

- Advancing the capabilities for rapid attribution—determining who instigated an attack so as to enable a timely and precise response.
- Understanding and measuring both direct and indirect effects of cyber attacks; assessing damages related to direct and indirect effects of cyber attacks.
- Determining whether a cyber operation is an attack or exploitation—or generally inferring intent.
- Trying to understand, through war game simulations, how social and technical systems in the Internet might respond to various attacks and provocations, how cyber attacks could escalate out of control, and which "games of cooperation" might best thwart attacks.
- Understanding the relationship between recovery time and value of an attack—an attacker is less motivated to take down a network if the victim can quickly restore it to operation.
- Finding effective means of planting or discovering Trojan horses and other forms of malware.
- Determining the effects of virtualization in the cloud on the ability to mount, detect, and thwart attacks.
- Understanding and minimizing risks introduced by development or use of cyber attack and exploit capabilities.
- Understanding and explaining implications of new technologies—how they might be attacked or how they might facilitate an attack or exploit. For example, technologies for smart grids, smart cars, wireless home networks, or social networking systems.
- Determining the requirements for getting good indications and warnings of cyber attack—is it necessary to penetrate adversary networks to get this in a timely enough manner to defend or respond effectively?

Studying these areas contributes to better defenses. It is not possible to build strong defenses without acquiring and maintaining a solid understanding of how attacks work and how effective they might be.

**It is not possible to build strong defenses without acquiring a solid understanding of how attacks work and how effective they might be.**

## What You Can Do

It is important that computing professionals bring their general knowledge of computers and networks to the discussions of technical, policy, legal, and social issues around cyber attack. There are several ways to do this:

- Engaging in research in the above areas and publishing results.
- Developing and participating in cyber attack and defense exercises; making sure that cyber exercises are true to technology and its limits.
- Participating in groups that address cyber attack issues, for example, the Cyber Conflict Studies Association (cyberconflict.org), which sponsors meetings and working groups on various topics relating to cyber attack and defense.
- Participating in online discussion groups such as the Cyber Security Forum Initiative's Cyber Warfare Division (CSFI-CWD) on LinkedIn.
- Participating in conferences such as InfoWarCon (cyberloop.org) or the Conference on Cyber Conflict sponsored by the NATO-accredited Cooperative Cyber Defence Centre of Excellence in Estonia (www.ccdcoe.org).
- Participating in government-sponsored working groups that address cyber attack issues.
- Separating truth from fiction about technology in media stories—writing articles that debunk myths.

Even though many of the meetings and discussions on cyber conflict emphasize the legal and policy issues, it is vital that computing professionals participate so that findings and recommendations are based on a sound understanding of technology. Moreover, the networks of computing professionals formed in these discussions become powerful resources for responding to cyber attacks.

We join with the NRC report to strongly endorse the strategy of openness in these efforts and discussions. Openness mobilizes many brains on difficult problems, increasing the chances of finding good solutions. C


**References**

1. Clarke, R., and R. Knake. *Cyber War.* Ecco, 2010.
2. Denning, D. E. *Information Warfare and Security.* Addison-Wesley, 1998.
3. National Research Council. *Technology, Policy, Law, and Ethics Regarding U. S. Acquisition and Use of Cyberattack Capabilities.* W.A. Owens, K.W. Dam, and H.S. Lin, Eds., National Academic Press, 2009. Available from MacArthur Foundation, macfound.org, search for "cyberattack."
4. Parnas, D. Software aspects of strategic defense systems. *Commun. ACM 28*, 12 (Dec. 1985), 1326–1335.
5. Vijayan, J. Over 75,000 systems compromised in cyberattack. *Computerworld* (Feb 18, 2010).



**Peter J. Denning** (pjd@nps.edu) is Distinguished Professor of Computer Science and Director of the Cebrowski Institute for Innovation and Information Superiority at the Naval Postgraduate School in Monterey, CA and is a past president of ACM.

**Dorothy E. Denning** (dedennin@nps.edu) is Distinguished Professor of Defense Analysis at the Naval Postgraduate School in Monterey, CA, and author of *Information Warfare and Security.*[2]